Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Hackers Exploit Zero-Day Flaw in EOL GeoVision Devices

Date of Publication	Last Updated Date	Admiralty Code	TA Number
November 18, 2024	May 14, 2025	A1	TA2024434

Summary

First Seen: November 14, 2024
Affected Product: GeoVision Devices
Malware: Mirai, LZRD
Impact: CVE-2024-11120 and CVE-2024-6047 are critical OS command injection vulnerabilities in outdated GeoVision devices, allowing unauthenticated attackers to execute arbitrary commands remotely. Actively exploited in the wild, it has been used by botnets, such as Mirai, for DDoS and cryptomining. With no patches available, users are advised to isolate or replace the devices urgently.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-11120	GeoVision Devices OS Command Injection Vulnerability	GeoVision Devices	✓	✓	✗
CVE-2024-6047	GeoVision Devices OS Command Injection Vulnerability	GeoVision Devices	✗	✓	✗

Vulnerability Details

#1

CVE-2024-11120 and CVE-2024-6047 are critical OS command injection vulnerabilities (CVSS 9.8) affecting multiple end-of-life (EOL) GeoVision IP surveillance devices. These flaws are present in the /DateSetting.cgi endpoint, where improper input validation, specifically in the szSrvIpAddr parameter, allows unauthenticated remote attackers to inject and execute arbitrary system commands.

#2

Both vulnerabilities are currently being exploited in the wild. Threat actors are using them to download and execute a Mirai-based malware variant known as LZRD, which transforms the compromised devices into nodes within a botnet. This botnet is primarily used for DDoS attacks and cryptomining, and the LZRD variant exhibits adaptations specifically designed to target vulnerable GeoVision systems. The attack vector requires no authentication or user interaction, making exploitation trivial for automated scanning and attack tools.

#3 The affected devices include GeoVision models such as GV-VS12, GV-VS11, GV-DSP LPR V3, and certain versions of GV-LX4C. Since these devices are EOL, no patches or updates are available to mitigate the flaw.

#4 It is recommended to disconnect these devices from the internet and replace them with supported alternatives. If replacement is not immediately feasible, they should be isolated within secure networks and closely monitored.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-11120	GeoVision VS12 GeoVision VS11 GeoVision DSP_LPR_V3 GeoVision LX 4 V2 GeoVision LX 4 V3	cpe:2.3:o:geovision:gvlx_4_v3_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gvlx_4_v2_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gv-vs12_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gv-vs11_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:geovision:gv-dsp_lpr_v3_firmware:*:*:*:*:*:*:*:*	CWE-78
CVE-2024-6047			

Recommendations

Immediate Isolation: The first step is to remove affected EOL GeoVision devices from the network. Alternatively, place them behind a properly configured firewall to prevent remote access. Block inbound connections to the /DateSetting.cgi endpoint at the firewall level, if device removal is not yet possible.

Device Replacement: Consider replacing these EOL devices with supported and up-to-date alternatives as soon as possible. Since these devices are no longer receiving patches or support from the manufacturer, replacement is crucial for long-term security.

Network Segmentation: If it is not feasible to remove the devices immediately, implement strict network segmentation. This approach limits their exposure and potential impact on other systems within the network.

Enhanced Monitoring: Implement enhanced monitoring for any suspicious activities or commands executed on these devices. Continuous monitoring can help in detecting unauthorized access attempts or exploitation attempts early.

Access Control: Strengthen access controls and authentication mechanisms for any networks where these devices are present. Ensure that only authorized personnel have access to these devices and their management interfaces.

Potential MITRE ATT&CK TTPs

TA0040 Impact	TA0042 Resource Development	TA0002 Execution	TA0001 Initial Access
TA0011 Command and Control	T1588.006 Vulnerabilities	T1588 Obtain Capabilities	T1588.005 Exploits
T1498 Network Denial of Service	T1496 Resource Hijacking	T1190 Exploit Public-Facing Application	T1071 Application Layer Protocol
T1071.001 Web Protocols	T1059 Command and Scripting Interpreter	T1584 Compromise Infrastructure	T1584.005 Botnet

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	209[.]141[.]44[.]28, 51[.]38[.]137[.]114, 176[.]65[.]144[.]253, 176[.]65[.]144[.]232, 198[.]23[.]212[.]246

TYPE	VALUE
SHA256	f05247a2322e212513ee08b2e8513f4c764bde7b30831736dfc927097baf6714, 11c0447f524d0fcb3be2cd0fbd23eb2cc2045f374b70c9c029708a9f2f4a4114, 8df660bd1722a09c45fb213e591d1dab73f24d240c456865fe0e2dc85573d85e, ecc794a86dcc51b1f74d8b1eb9e7e0158381faadaf4cb4ee8febd4ba17fd2516, 03b1506c474a6f62f2e2b73ba4995b14da70b27e6d0aaea92638197e94d937c3, 0333c6ac43c6e977e9a1c5071194d3cf8aa01222194c6e7f2fd13e631d03522d, 7a8a46ace3b9261c2c7a399dcae037ce4f185f52f94b893d5bc00cd1228fb13a, 50c5b6c971c503240b91787d31f9314ded38d4f2700ff90deb032478b30aa0c5, bb2ab0879282c5c7f92a51e6482d3eb60a84ab184eca258ea550d9ed04bc5eda, 074a261bf281da36cc91cd13f86c7a8f75fdf96807d525c24b22c48fe01584a3, 5e721c013a6e8b2246aae86974f2163d3b57a7e6608a318ab84c44b1650e650a, de3c9ecb51564e4298ce7e4ff749be0a42d37824d2fd3d5b7fbab86a04105b88, aaba1ce1f182122a7ea05683623ab2d9bd05a3507e0dfc95e8e4165f629f80a8, 3f465182b5c594784e406a6a5de2f398bcc2e2ffc92d049a7990f37c267550a6, 3d6a544b1f03df23e734a65b9f1e808ff513ad881f09745a3959d696075c057e, 5180e3050a4a5cff52dcd8e8bb39fb6cf59a264a8fb6ddcc239615b340f1b99a, 2cc4d952856a8f2e1dd73b175d730d9cc7a04c73cf6452c8d0411eedf3aed5d5, dc21419b73566651b4c1e85879c0c98a4dcff8f7d206d9a978822000503658e9c, 866b2dbbd1978be007460835e8f3d2e02c1b321f856a18ba3e53030d4effe69a, 64ca8dd1a2702e0463bab19a0b826f79c55cfd46e4e1b41c6c33d7e7aa2c7530, 9f05425478d03e4a2fd5b990fe5625d93c468b80a3880bb52475aa7561548582, bf6984ccc9fb21beba3f492420901be0b0bace8d4530e6d2850f039622f1b96f, 58f7d61e3e474d5f5eccbba79556070220f52fa011b7cd24bdd96c23c338cd4b

TYPE	VALUE
Domain	connect[.]antiwifi[.]dev

Patch Details

No patch is available for CVE-2024-11120 or CVE-2024-6047, as it affects end-of-life GeoVision devices with no vendor support; users must replace or isolate the devices to mitigate the risk.

References

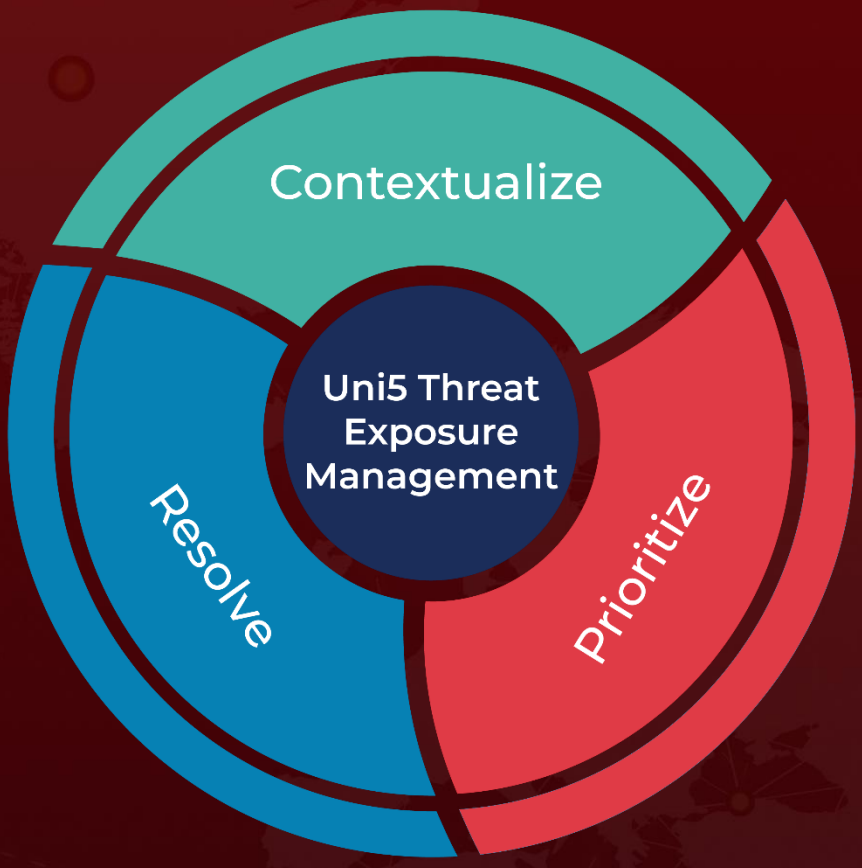
https://www.twcert.org.tw/en/cp-139-8237-26d7a-2.html

https://www.akamai.com/blog/security-research/active-exploitation-mirai-geovision-iot-botnet

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 18, 2024 . 6:30 AM

More at www.hivepro.com